AD-A264 238

(2)



STUDY PROJECT

# MULTILEVEL SECURITY: HOW IT FITS IN THE STRATEGIC VISION "C4I FOR THE WARRIOR"

BY

LIEUTENANT COLONEL GREGORY S. HOLLISTER
United States Air Force



DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1993

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

# REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

| | |
|---|---|
| 1a. REPORT SECURITY CLASSIFICATION<br>Unclassified | 1b. RESTRICTIVE MARKINGS |
| 2a. SECURITY CLASSIFICATION AUTHORITY | 3. DISTRIBUTION/AVAILABILITY OF REPORT<br>Approved for public release. Distribution is unlimited. |
| 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE | |
| 4. PERFORMING ORGANIZATION REPORT NUMBER(S) | 5. MONITORING ORGANIZATION REPORT NUMBER(S) |
| 6a. NAME OF PERFORMING ORGANIZATION<br>U.S. ARMY WAR COLLEGE<br>6b. OFFICE SYMBOL (If applicable) | 7a. NAME OF MONITORING ORGANIZATION |
| 6c. ADDRESS (City, State, and ZIP Code)<br>ROOT HALL, BUILDING 122<br>CARLISLE. PA 17013-5050 | 7b. ADDRESS (City, State, and ZIP Code) |
| 8a. NAME OF FUNDING/SPONSORING ORGANIZATION<br>8b. OFFICE SYMBOL (If applicable) | 9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER |
| 8c. ADDRESS (City, State, and ZIP Code) | 10. SOURCE OF FUNDING NUMBERS<br>PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO. |

11. TITLE (Include Security Classification)
MULTILEVEL SECURITY: HOW IT FITS IN THE STRATEGIC VISION "C41 FOR THE WARRIOR"

12. PERSONAL AUTHOR(S)
Lt Col Gregory S. Hollister, USAF

| 13a. TYPE OF REPORT | 13b. TIME COVERED | 14. DATE OF REPORT (Year, Month, Day) | 15. PAGE COUNT |
|---|---|---|---|
| Individual | FROM ______ TO ______ | 93 February 5 | 26 |

16. SUPPLEMENTARY NOTATION

| 17. COSATI CODES | | | 18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) |
|---|---|---|---|
| FIELD | GROUP | SUB-GROUP | |
| | | | |
| | | | |


19. ABSTRACT (Continue on reverse if necessary and identify by block number) "The downsizing of military forces and the shrinking defense budget have resulted in increased reliance on C41 interoperability. The C41 for the Warrior concept starts with the warrior's requirements and provides a roadmap to reach the objective of a seamless, secure, interoperable global C41 network for the warrior. The C41 for the Warrior concept will give the battlefield commander access to all information needed to win in war and will provide the information when, where and how the commander wants it." These are the words of General Colin L. Powell, Chairman of the Joint Chiefs of Staff. They reflect his views on the importance of Command, Control, Communications, Computer, and Intelligence (C41)and its increased importance in future confrontations on the battlefield. The C41 for the Warrior concept's focus is on making the operational commander's job easier. One facet of that approach is allowing the warrior to request or "pull" only the information required at a particular time. This will prevent the warrior from being inundated with multiple reports, from multicple sources, requiring extensive analysis and deconfliction wasting precious decision time. "Pulling" this information from multiple sources and "fusing" (over)


| | |
|---|---|
| 20. DISTRIBUTION/AVAILABILITY OF ABSTRACT<br>☐ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS | 21. ABSTRACT SECURITY CLASSIFICATION |
| 22a. NAME OF RESPONSIBLE INDIVIDUAL<br>WALTER C. INGRAM, COL, SC | 22b. TELEPHONE (Include Area Code) 717-245-3032 / 22c. OFFICE SYMBOL AWCAC |

DD Form 1473, JUN 86 Previous editions are obsolete. SECURITY CLASSIFICATION OF THIS PAGE

it into one simple report for the operational commander has significant security implications. This study examines the C4I for the Warrior concept, multilevel security, and accreditation of computer networks. It is an attempt to understand what problems lie ahead in the effort to incorporate multilevel security into the C4I for the Warrior concept and provide recommendations addressing those problems.

USAWC MILITARY STUDIES PROGRAM PAPER



# MULTILEVEL SECURITY:

# HOW IT FITS IN THE STRATEGIC VISION "C4I FOR THE WARRIOR"

by

Lieutenant Colonel Gregory S. Hollister
United States Air Force

Colonel Walter C. Ingram
Project Adviser



U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

## ABSTRACT

AUTHOR: Gregory S. Hollister, Lt Col, USAF

TITLE: Multilevel Security: How it Fits in the Strategic Vision "C4I for the Warrior"

FORMAT: Individual Study Project

DATE: 5 February 1993 PAGES: 26 CLASSIFICATION: Unclassified

"The downsizing of military forces and the shrinking defense budget have resulted in increased reliance on C4I interoperability. The C4I for the Warrior concept starts with the warrior's requirements and provides a roadmap to reach the objective of a seamless, secure, interoperable global C4I network for the warrior. The C4I for the Warrior concept will give the battlefield commander access to all information needed to win in war and will provide the information when, where and how the commander wants it." These are the words of General Colin L. Powell, Chairman of the Joint Chiefs of Staff. They reflect his views on the importance of Command, Control, Communications, Computer, and Intelligence (C4I) and its increased importance in future confrontations on the battlefield. The C4I for the Warrior concept's focus is on making the operational commander's job easier. One facet of that approach is allowing the warrior to request or "pull" only the information required at a particular time. This will prevent the warrior from being inundated with multiple reports, from multiple sources, requiring extensive analysis and deconfliction wasting precious decision time. "Pulling" this information from multiple sources and "fusing" it into one simple report for the operational commander has significant security implications. This study examines the C4I for the Warrior concept, multilevel security, and accreditation of computer networks. It is an attempt to understand what problems lie ahead in the effort to incorporate multilevel security into the C4I for the Warrior concept and provide recommendations addressing those problems.

## LIST OF ILLUSTRATIONS

## INTRODUCTION

"At the height of the Persian Gulf conflict, the automated message information network passed nearly 2 million packets of information per day through gateways (computer networks) in the Southwest Asia theater of operations. Efficient management of information increased the pace of combat operations, improved the decision making process, and synchronized various combat capabilities. The technology developed to support these networks proved to be a vital margin that saved lives and helped achieve victory."[1]

Increased reliance on Command, Control, Communications, Computer, and Intelligence (C4I) systems is a fact of life. As we downsize the military, C4I will become even more crucial to ensuring we provide the right force, at the right place, at the right time. More directly, effective C4I is absolutely essential to support our National Military Strategy. "One of the essential elements of our national military strategy is the ability to rapidly assemble the forces needed to win -- the concept of applying decisive force to overwhelm our adversaries and thereby terminate conflicts swiftly with a minimum loss of life."[2] The concept of C4I for the Warrior provides the proper focus on the warrior and the methods of applying C4I to support the warrior in the most effective manner possible.

The purpose of this paper is to examine how C4I for the Warrior (C4IFTW) can be implemented securely across service boundaries thereby supporting the National Military Strategy. The paper will look first at the C4IFTW concept. Next, it will discuss the meaning of multilevel security (MLS). This will be

followed by a discussion on accreditation of computer systems. The final section will deal with integrating multilevel security into the C4IFTW concept and provide recommendations on policy and technology to ensure we keep the proper focus on the warrior.

## A NEW MILITARY STRATEGY

As overall force levels draw down and forward-deployed forces shrink, our ability to project our power will underpin our strategy more than ever. We must be able to deploy substantial forces and sustain them in parts of the world where prepositioning of equipment will not always be feasible, where adequate bases and infrastructure may not be available to support our forces once they arrive.[3] Our strategy of the "come-as-you-are" arena of spontaneous, often unpredictable crises, requires fully-trained, highly-ready forces that are rapidly deliverable, and initially self-sufficient.[4] Therefore, C4I systems must become an integral part of a strategy to ensure effective command and control and integration of rapidly deployed force packages.[5] This is where the concept of C4IFTW fits in so well.

## C4I FOR THE WARRIOR(C4IFTW): ITS GENESIS

A short time after his arrival as Director, Command, Control, Communications and Computer Systems (J-6), Joint Staff, VADM Richard C. Macke began to develop a concept to focus C4I around the "warrior". He fleshed out a paper underscoring the need for interoperability and defining the warrior's requirement for a "ground truth" picture of assigned battle space. This "ground truth" would allow the warrior to order, respond and coordinate horizontally and vertically to the degree necessary to prosecute his warfighting mission in that battle

[6] space. This concept had to be focused from a C4I perspective and the capability C4I could provide to enhance the warrior's knowledge of "ground truth". As a result, the Vice Director J-6, Major General Albert J. Edmonds, formed a "task force" to flesh out this concept with a focus on C4I systems and architectures in place with an eye toward the future. The author was a member of that initial team.

The team's task was to take VADM Macke's concept, brainstorm what it meant and could mean, and present those thoughts to VADM Macke in a briefing to ensure we were on the right track. The two week effort culminated with a direction to proceed from the Admiral along with the establishment of a new division within J-6 to formalize the concepts in the Admiral's paper and the briefing. The new division is the Architecture and Integration Division. This division began the arduous task of reviewing all known C4I architectures throughout the Department of Defense (DOD) and using that review to establish how to go about developing a warrior-focused C4I architecture for all CINCs, Services, and Defense agencies to use in developing and employing C4I systems. The major tenets of that architectural concept will be described in the following paragraphs.

## C4IFTW: A STRATEGIC VISION IN C4I

C4IFTW sets forth a concept of guiding principles and provides a roadmap for achieving global C4I interoperability that:

- will allow any Warrior to perform any mission, any time, any place
- is responsive, reliable, and secure
- is affordable

The concept provides an interoperable, fully integrated C4I system for our warriors to assess, respond, lead, and fight:

- with maximum effectiveness
- on arrival
- in unison with any other element.

It will bring to the warriors:

- accurate and complete pictures of their battlespace
- timely and detailed mission objectives
- the clearest view of their targets.[7]

Intensive analysis revealed there was no single, overarching C4I architecture from which all supporting Commander in Chief (CINC), Service, or Defense agency C4I architectures could be modeled. As a result, a unifying concept was essential to achieving the objective of a global C4I system that would support the requirements of the warfighter, consistent with national security plans. Through a revolutionary approach and in an evolutionary manner, this concept addresses joint force operational C4I interoperability issues. It can improve the joint warfighter's ability to manage and execute crisis and contingency operations and provide a means for unifying the many heterogeneous service C4I programs currently being pursued. The concept has four major components that are critical to understanding how it can help the warfighter lead more effectively within the confines of his battlespace and assigned mission. These components are fusion, infosphere, preplanned essential elements of information (P2E2I), and over the air updating (OTAU).[8]

The first of the four components that will be discussed is fusion. As

addressed earlier, one of the purposes of C4IFTW is to tailor information for the warrior and allow the warrior to "pull" the required information when it is needed. This will minimize, and hopefully eliminate, inundation of the warrior with information from multiple sources. Fusion is one method to eliminate this inundation. Fusion is the process of receiving and integrating all-source, multimedia and multiformat information. It produces and makes available an accurate, complete summary.[9] This summary is as timely, more concise, less redundant, and more useful to the warrior than if the same information were received directly from separate multiple sources. In effect, the warrior requests the information that is fused from an "infosphere". A clearer understanding of the infosphere is needed to fully grasp this concept.

The infosphere contains the total combination of information sources, fusion centers, and distribution systems that represent the C4I resources a warfighter needs to pursue his operational objectives.[10] The warrior essentially plugs in to the infosphere and pulls out the required information when needed providing timely and relevant information. The request goes out to any and all sources within the infosphere to acquire information related to the request. That information is condensed in a single update to the warrior to give him only the information required in the format required with little or no need for human evaluation and no confusion from conflicting information from multiple sources.

Due to the stated position of the National Military Strategy, the warrior must be ready to fight on arrival. Therefore, warriors need certain types and amounts of information with them for their systems or they must be able to access

the infosphere immediately upon commencement of an operation. The warrior must take some of this information to the battlefield and thus minimize time to become fully operational within theater.

Taking some information to the battlefield will minimize the warriors dependence on the infosphere. The warrior must plan ahead to determine what elements of information are required upon arrival in anticipation that hostilities may begin immediately. This information is described as preplanned essential elements of information (P2E2I). P2E2I is all of the relevant information the warrior anticipates that will be needed to plan and carry out a future mission. This information will comprise the initial, static database. As the warrior progresses toward and into combat, this data will be refreshed and supplemented automatically from decentralized elements of the infosphere.[11] Once contact is made with the enemy, the battlespace changes as does the need for the warriors information. Any information that has been brought to the battlefield will need updating.

Over-the-Air- Updating (OTAU) is the process by which the warrior's data-bases are automatically updated by elements of the infosphere.[12] An example of this may be a technical order (maintenance manual) change to an M-1 tank. The M-1 technical order will be placed on a computer chip within the tank to minimize lift requirements - no paper tech orders. An updated order in the factory could be loaded into a sustaining base computer. The computer could automatically transmit the change only information into the infosphere and to the warrior at the distant end. This would automatically update the tank's technical order computer

chip. This ensures the warrior's force has the most current information available to take the fight to the enemy while making lift space available for additional ammunition and other supplies by eliminating the need to ship paper technical orders to the front.

C4IFTW focuses on the information needs of the warrior. It changes the paradigm on how information is deployed and how the battlespace is presented to the warrior. This concept fits well with the need for total interoperability between the services and supports the strategy of a rapidly deployable contingency force to counter regional crises. Being able to provide this architecture in a secure fashion is tremendously difficult.

## THE DEFENSE DATA NETWORK - AN EXAMPLE OF HOW MULTILEVEL SECURITY CAN HELP

The Defense Data Network (DDN) has been the primary means of computer communications for DOD since 1983. As the Joint Staff Integrated Data Communications Officer from 1990 until 1992, the author became intimately familiar with DDN.

The DDN was established with four separate networks for security reasons. The Military Network (MILNET) transports UNCLASSIFIED but SENSITIVE (U) information, Defense Secure Network 1 (DSNET1) transports SECRET (S) information, Defense Secure Network 2 (DSNET2) transports the TOP SECRET (TS) information of the Worldwide Military Command Control Communications System (WWMCCS) computer network, and Defense Secure Network 3 (DSNET3) transports TOP SECRET SPECIAL COMPARTMENTED

INFORMATION (TS/SCI) for the Defense Intelligence Agency.

Each network requires separate computers that are cleared to process information for that particular network. A warfighter needing access to the TS/SCI network and the U network would have to operate and maintain two separate computer systems and pay to support two separate, DSNET3 and MILNET, communications networks. Warfighters needing access to all four levels of information would need to support four different computer systems and four different networks. This is called the "swivel chair" effect.

This situation of multiple computer systems and multiple communications networks is intolerable for several reasons. Multiple systems are costly. Four times as many systems must be acquired and maintained, eating up acquisition and operation funds. Multiple acquisitions also mean multiple acquisition efforts. Depending on the dollar threshold, the same process for acquiring one computer system may be repeated many times over merely because different systems must operate at different and separate classification levels for security reasons. This is a huge investment in manpower at all levels up to and including the Vice Chairman of the Joint Chiefs of Staff as chairman of the Joint Requirements Oversight Council (JROC).

Expenditure of monetary and manhour resources is not the only drawback. The warfighter's ability to gather and assimilate information from the multiple sources becomes limited at best with the definite possibility of information overload occurring. Multilevel security is required to eliminate this duplicative and inefficient operational configuration.

## MULTILEVEL SECURITY - WHAT IS IT AND WHAT DOES IT DO?

A computer operating in a multilevel security mode is operating in an environment in which two or more classification levels of information are processed simultaneously even though some users (even only one) are not cleared for all levels of information processed.[13] A multilevel network is one in which some users do not have the clearance for all information processed. This network may comprise a mixture of dedicated and multilevel components, where two or more differ in their classifications and some users do not have all access approvals.[14]

If multilevel security is implemented appropriately at the computer systems and communications networks levels, then all separate computer networks can be merged into one, processing all levels of information simultaneously. This drastically reduces costs for multiple acquisitions, separate systems operations, and minimizes the "swivel chair" effect mentioned earlier. As an example, the four separate computer and communications networks of DDN could be merged into one multilevel computer and communications system:

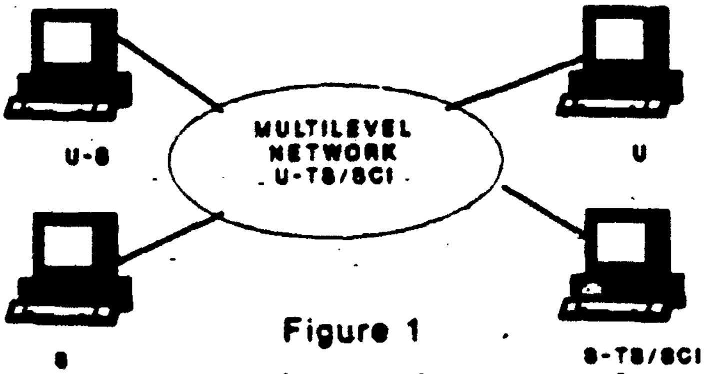


Figure 1

Multilevel security not only allows for the merging of separate systems processing various levels of classified information, it will also assist the warfighter

in his effort to "pull" and "fuse" information.

Pulling and fusing information will make the warfighter's job easier. The warfighter may request the latest battle readiness status of friendly forces in friendly battlespace. The query will be entered into the warfighter's single entry device and be sent into the worldwide computer and communications system called the infosphere. The query may require information be "pulled" from computer systems and their databases ranging in classification of UNCLASSIFIED for parts availability to SECRET for forward line of troops location to SPECIAL COMPARTMENTED INFORMATION for special forces preparing to jump off behind enemy lines. The infosphere collects all available data and then sends it to a fusion point to be reduced to a graph or chart that is readily usable to the warfighter. An example of this process is shown in the following figures.

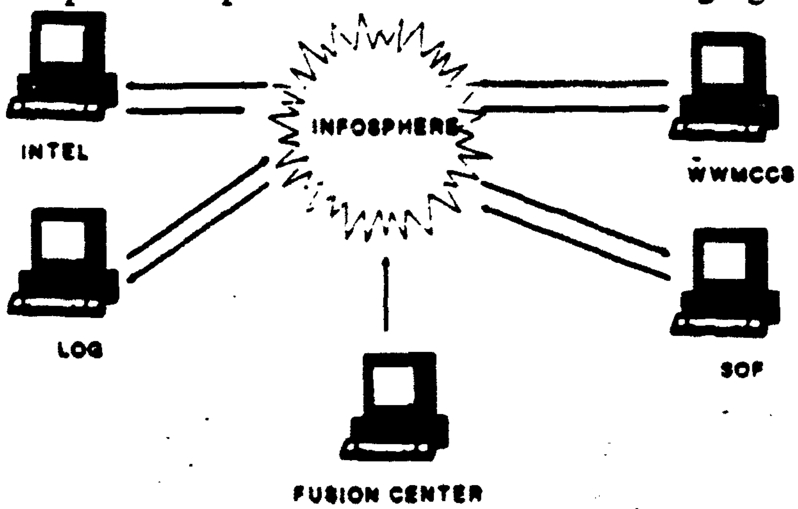


Figure 2

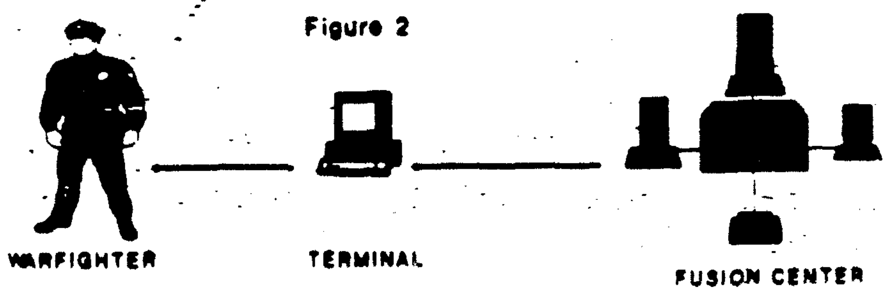


Figure 3

Understanding the C4IFTW concept is not enough. It must be implemented securely. Understanding how computer security is established is paramount to incorporating MLS into C4IFTW.

## ACCREDITATION AND CERTIFICATION

The concept of C4IFTW has been defined along with the meaning of multilevel security. We next need to understand how a system is approved to operate in the multilevel security mode. A discussion of technical assessment, risk analysis, and the role of approving system operation is in order.

Department of Defense (DOD) policy states that any computer system, more commonly referred to as an automated information system (AIS), that processes classified, sensitive unclassified, or unclassified information must undergo a technical assessment and management approval before it is allowed to operate.[15] The technical assessment establishes the extent to which the system meets a set of specified security requirements for its mission and operational environment. The approval formally assumes responsibility for operating at an acceptable level of risk. The technical assessment and management approval processes are called certification and accreditation, respectively. A Designated Approving Authority (DAA) grants the approval to operate based on recommendations resulting from the technical assessment.[16]

Approval to operate is the official management authorization to operate an AIS: (a) in a particular security mode; (b) with a prescribed set of countermeasures (e.g., administrative, physical, personnel, communications, emissions, and

computer security controls); (c) against a defined threat and with stated vulnerabilities and countermeasures; (d) with a given operational concept; (e) with stated interconnections to other AISs; (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility; and (g) for a specified period of time.[17]

The comprehensive technical assessment of a system's security, made in support of the accreditation process, that establishes the extent to which a particular system meets a set of specified security requirements for its mission and operational environment, is the risk assessment. This should result in identifying residual risk as well as a recommendation to the Designated Approving Authority.[18]

The process of identifying and analyzing threats and vulnerabilities associated with an information system, to determine the risks (potential for losses) and to identify cost-effective corrective measures is risk analysis. Risk analysis is part of risk management, which is used to minimize risk by specifying security measures commensurate with the relative values of the resources to be protected, the vulnerabilities of those resources, and the identified threats against them. The method should be applied throughout the system life cycle. When applied to system design, a risk analysis aids in countermeasure specification. When applied during the implementation phase or to an operational system, it can verify the effectiveness of existing countermeasures and identify areas in which additional measures are needed to achieve the desired level of security.[19]

As a part of the technical evaluation process, integrity of information is a critical factor. This pertains to ensuring that data continues to be a proper

representation of information, and that information processing resources continue to perform correct processing operations. Another objective is to ensure that information retains its original level of accuracy. Data integrity is that attribute of data relating to the preservation of its meaning an completeness, the consistency of its representations, and its correspondence to what it represents. System integrity is that attribute of a system relating to the successful and correct operation of computing resources.[20]

The official who has the authority to decide on accepting the security countermeasures that will provide an appropriate level of data and system integrity prescribed for an AIS or the official responsible for issuing an accreditation statement that records the decision to accept those countermeasures is the Designated Approving Authority (DAA). The DAA must be at least at the Wing or Brigade level, have authority to evaluate the overall mission requirements of the AIS, and provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS. When there are multiple systems that must interconnect, there are multiple accreditors. In these situations the sharing of responsibilities for approving system interconnection and operation must be carefully defined in a Memorandum of Agreement (MOA). The DAA makes a determination on whether or not to allow system operation based on an assessment of operational need versus risk. The system is then approved for operation, with or without stipulations, but in any event must be revaluated in most cases within a three year period.[21]

## ACCREDITATION AND CERTIFICATION ISSUES

The process of accreditation and certification is both complex and cumbersome. It is paramount that the process take place to ensure proper protection of computer systems and the information they contain. Problem areas in the process need to be highlighted.

Policy has been unable to keep up with rapidly advancing technology. For example, current policy provides little guidance for the range of systems employed today. This range includes everything from large, central computer facilities to stand-alone personal computers or intelligent workstations often tied together over local area networks (LANs) or connected via complex networks. This situation of lagging policy is unacceptable if the concept of C4IFTW is to work. Project managers have been unable to fully implement systems in the required operational configuration due to inadequate or non-existent security policy for system development. A program manager begins system fielding and is directed to cease because sufficient security mechanisms are not in place. Unfortunately, there is no consolidated policy for development of the system.

The systems mentioned above have significant differences in functionality and vulnerabilities, and current policy provides little guidance to DAAs on determining an acceptable level of risk based on the technology, environmental factors, and operational requirements. Improved guidance is needed on how to certify and accredit all types of systems: networks, distributed systems, systems with integrated workstations, database management systems, and, in particular,

multilevel secure systems. Current policy is often inconsistent across DOD components. These inconsistencies may cause difficulties as many individually certified accredited systems from multiple components are being integrated into a larger system. DOD has no clear, consolidated security guidance and there is no institutionalized training for DAAs, certification technicians, or computer system administrators.[22]

There are many reasons for these problems. One reason is the lack of resources, both staffing and dollars, to perform certification and accreditation. Another reason for not certifying systems relates to the question of what is a reasonable effort for certification. Another area not addressed by current policy is the associated consequences of not accrediting a system. Many systems are operating today without accreditation and there is no enforcement mechanism in place to ensure this problem is corrected. Until DOD ensures all computer systems are properly accredited, they are vulnerable to exploitation. Even if DOD identifies these non-secure systems, there are no resources to make the corrections.[23]

The final accreditation and certification issue to be addressed is acceptable level of risk. Part of the accreditation decision is the acceptance of a given level of risk against a defined threat. The DAA must balance the risk of disclosure, loss or alteration of information, the availability of the system based on the vulnerabilities identified by the certification process, and the threat that these vulnerabilities may be exploited in the specific environment in which the system is being used.

With regard to threat, DAAs in general are not sufficiently aware of specific

national, regional, and environmental threat data that is needed to make decisions regarding acceptable risk. Risk must also be balanced against operational requirements mandating acceptance of higher risk, such as during a crisis situation. An example is a command that requires high-speed data transfer between systems with differing security levels. MLS functionality is needed, but the technology to support it is not available. A real-world situation that needs to be addressed by policy follows.[24]

## THE ARMY TACTICAL PACKET NETWORK:
## A STUDY IN MLS FRUSTRATION

The explosion of computer technology development and its use on the battlefield called for the extension of DDN and all computer systems it supports to the battlefield (echelons Corps and below). Congressional direction to ensure tactical forces have computer communications networks similar to DDN within theater and access to DDN out of theater, highlight the visibility and level of commitment to ensure computer system access for the warfighter.[25]

The Army's approach to providing this capability is to include packet data communications equipment similar to that used in DDN in their tactical communications system, Mobile Subscriber Equipment (MSE - essentially a tactical cellular telephone system that provides both voice and data/computer communications capability). This effort is named the Tactical Packet Network (TPN).[26]

The warfighter requires access to computer systems located at sustaining

bases to order supplies, gather intelligence information, and send/receive messages to name just a few applications. This requirement calls for an automated interface between the TPN and DDN which will allow the warfighter to exchange information with the sustaining base environment. The focus is on developing a solution that will not place the burden for the TPN to DDN connection on the warfighter.[27]

The currently approved TPN security configuration does not satisfy all warfighting requirements. When initially conceived, the TPN was to operate at the SECRET level only. This is the same classification level at which MSE operates. Unfortunately, this configuration does not address a major Army requirement - to connect to the UNCLASSIFIED portion of DDN, MILNET.

Operations DESERT SHIELD and DESERT STORM clearly demonstrated the need for connectivity from the tactical level back to the sustaining base for information such as parts ordering or status, pay record information, health data bases for treating illnesses, etc. The computer systems that provide this information are on the MILNET. Therefore, the Army has a requirement to connect their tactical computer systems to the SECRET and UNCLASSIFIED portions of DDN simultaneously to support the warfighter at both the strategic and operational levels.[28]

Simultaneous connections to UNCLASSIFIED and SECRET systems creates a significant security problem. While the MLS concept would allow such a connection, the technology and policy do not yet exist to implement this configuration of computer networks. One of the greatest security threats from this

type of connection comes from computer system intruders, commonly referred to as "hackers". Hackers are very much like the young boy in the movie "War Games" that broke in to the computer system controlling the nation's nuclear missiles. Hackers employ rudimentary computer skills and public networks trying to gain access to a computer system that uses poor, if any, computer security mechanisms. Once in these systems, hackers can plant computer programs called viruses that can erase data files completely or insert commands that will tell the computer to send specific information to them automatically whenever it is entered into the system.

This risk is real. In the book The Cuckoos Egg, author Cliff Stoll describes how he captured a computer spy ring in Hanover, Germany breaking in to United States government computers. These computer spies had access to systems such as those at White Sands Missile Range, Space Systems Division, and Redstone Arsenal. The hackers gained access to these systems through a connection between the UNCLASSIFIED portion of DDN, MILNET, and the general public's computer network systems. This global networking of computer systems is commonly referred to as the INTERNET.[29]

While the risk is real, the need for connecting government and public sector computers is real as well. This connection is required for government computers to communicate with computers supporting commercial transportation enterprises such as rail, trucking, and shipping. In addition, DOD research laboratories use the connection to exchange information with civilian counterparts that are on contract to assist in DOD programs. The risk was deemed acceptable until the requirement

to simultaneously connect networks processing different classifications of information arose.

The Army has a real need to connect its TPN to both the SECRET and UNCLASSIFIED networks of DDN. Cost constraints prohibit funding of two networks, one that would process UNCLASSIFIED information and the other that would process SECRET information. Therefore, while the Army is trying to move in the direction of C4IFTW, the lack of MLS technology, focused and properly coordinated DOD policy and procedures in the field prevents simultaneous connections between SECRET and UNCLASSIFIED networks. The only real solution is to connect to only one DDN system and relay information to the other by hand as shown in the figure below:

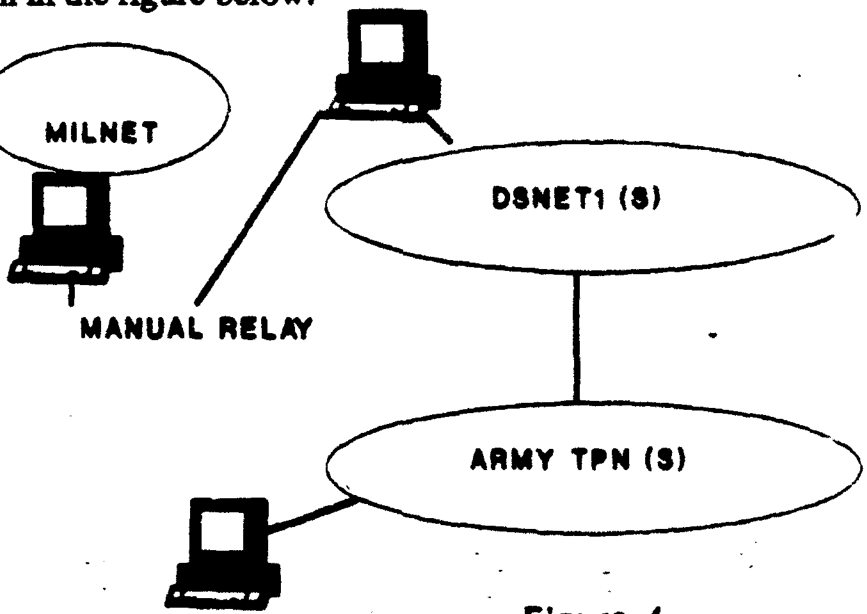


Figure 4

WHAT NEEDS TO BE DONE?

Clear and focused initiatives facilitating rapid employment of current technology with an eye toward evolution are required. Required initiatives can be broken down into three main categories of MLS technology insertion, training, and

security guidelines and improvements.

While on the Joint Staff the author worked closely with the author of the MLS Target Architecture and Implementation Strategy. The major focus of this document, in the near term, is technology insertion at two Unified Command locations - United States Transportation Command (USTRANSCOM) and United States Central Command (USCENTCOM). MLS technology is being inserted into the AIS systems supporting the two Unified Command headquarters. While Unified Command focus is essential to supporting the warfighting mission, it does not require MLS insertion be limited to Unified Command headquarters.

RECOMMENDATION: MLS technology implementation in existing communications-computer systems must remain focused on the warfighter but not limited to the Unified Command headquarters locations identified above. The MLS program office at the Defense Information Systems Agency (DISA) must take the lead to map out where and how emerging MLS technology may be employed at echelons Corps and below in the Army and equivalent levels in other Services. DISA, in consultation with the National Security Agency (NSA), the Joint Staff, and the Army should map out how existing and emerging MLS technology can be used to satisfy the Army requirement to connect the TPN simultaneously to SECRET and UNCLASSIFIED networks. This effort will include architecture, policy, and procedure development as well as methods for accreditation and certification. Other systems to be included are the Integrated Tactical-Strategic Data Network and the Defense Message System. This effort should be completed NLT 1 September 1993.

Training is another area where increased emphasis will enhance DOD's ability to incorporate MLS into the C4IFTW concept. There is no standardized requirement for training of DAAs or certification technicians across DOD to ensure all understand how to best evaluate the security posture of an AIS.

RECOMMENDATION: The Defense Information Systems Security Program (DISSP) in conjunction with NSA, DIA, the Joint Staff, DISA and the Services and Defense agencies, should develop training modules for agencies and individuals responsible for system accreditation and certification. Training programs will vary in length and level of intensity ranging from broad, overarching requirements for DAAs to very specific and technically oriented training for system certifiers. This training must be institutionalized to ensure system and informational integrity are not jeopardized as we interconnect systems processing information of differing security levels. Training programs are to be in place no later than 1 September 1993. Modules will be developed for levels of responsibility ranging from the President to the security officer for individual workstations.

The third and final major area to be addressed is security guidelines. As DOD began connecting the UNCLASSIFIED portion of DDN with the TOP SECRET DOD messaging system (AUTODIN) many questions on how to make the secure connections arose. Given the lack of specific guidance, the Defense Message System Security Policy Working Group (SPWG) took on the task to draft such guidance and structure a process to ensure the connections were made with an acceptable level of risk.

RECOMMENDATION: The DISSP should take on the task to clearly delineate what the technical and procedural policies are to make such connections securely and what actions are required in all stages from concept to implementation to satisfy these requirements. To date, all efforts have focused only on the Defense Message System and do not provide a general, broad-brush approach. Guidance must be developed and distributed for all possible AIS connections no later than 1 September 1993.

## CONCLUSION

Operations DESERT SHIELD and DESERT STORM clearly demonstrated our need for effective C4I to mass force and defeat an enemy swiftly and decisively. Our new national strategy will be implemented in an environment of dwindling defense dollars ,declining force structure, and the use of forward presence versus forward deterrence. This environment will make a swift, decisive victory an even more difficult task for U.S. forces to achieve. The concept of C4IFTW and its focus on warfighting are paramount to maximizing use of what resources will remain after budget cuts and force restructuring.

The concept of C4IFTW will remain just that, a concept, unless MLS technology can be inserted into existing systems to facilitate fusion of information and formation of the warrior's ground truth picture of battlespace. Without MLS, the warfighter will not be able to pull information and have it shaped and presented promptly and in a format easily understood. Implementation of the three recommendations in this paper will begin implementation of MLS into existing systems and evolution toward the C4IFTW concept.

## ENDNOTES

1. The Joint Staff, C4I for the Warrior, Joint Staff Pamphlet (Washington: The Joint Staff, 12 June 1992), 1.

2. The Joint Staff, National Military Strategy of the United States, Joint Staff Pamphlet (Washington: The Joint Staff, January 1992), 10.

3. The White House, National Security Strategy of the United States, White House Pamphlet (Washington: The White House, August 1991), 29.

4. The Joint Staff, National Military Strategy of the United States, 23.

5. The Joint Staff, Annex C, National Military Strategy Document, CM-1309-92 (Washington: The Joint Staff, 19 June 1992), V-H-1.

6. VADM Richard C. Macke, "Command, Control, Communications and Computers (and Intelligence) for the Warrior," Joint Staff Draft, 27 March 1992, 2.

7. The Joint Staff, C4I for the Warrior, 2.

8. Ibid., 3.

9. Ibid.

10. Ibid.

11. Ibid., 5.

12. Ibid., 6.

13. Department of the Army, "The Current Multilevel Secure (MLS) Architecture Initiatives and the Impact of the TPN-DDN Interface Solution on Battlefield Automated Systems (BAS's)," US Army Briefing (Ft. Gordon, Georgia: US Army Signal Center, 26 June 1992), 12.

14. Ibid.

15. A.R. Friedman and I. M. Olson, Introduction to Certification and Accreditation Concepts, Draft Document (McLean, Virginia: National Security Agency, June 1992), 1.

16. Ibid.

17. Ibid., 5.

18. Ibid., 6.

19. Ibid., 11.

20. Ibid., 10.

21. Ibid., 8.

22. Ibid., 21.

23. Ibid., 22.

24. Ibid.

25. Major James Kohlmann, TPN-DDN Functional Requirements Document Coordinating Draft, Army document (Ft. Gordon, Georgia: US Army Signal Center, 22 June 1992), 2.

26. Ibid.

27. Ibid.

28. Ibid., 1.

29. Cliff Stoll, The Cuckoo's Egg (New York: Simon and Schuster, 1990)

## BIBLIOGRAPHY


Boger, Jeffrey, Commander, United States Navy. Interview by author, 29 October 1992, Pentagon, Washington, D.C., Notes taken.

Brohm, Gerard P., Brigadier General, United States Army. "Proposed Changes to the Multicommand Required Operational Capability (MROC) 3-88, the Defense Message System (DMS)." Memorandum for the Joint Chiefs of Staff, J6. Washington, 24 August 1992.

Brundidge, Gregory, Major, United States Air Force. Interview by author, 29 October 1992, Pentagon, Washington, D.C., Notes taken.

Defense Intelligence Agency. Joint Worldwide Intelligence Communications System (JWICS) Evolutionary Design and Plan. Washington: Defense Intelligence Agency, 22 June 1992.

Department of the Army. "The Current Multilevel Secure (MLS) Architecture Initiatives and the Impact of the TPN-DDN Interface Solution on Battlefield Automated Systems (BAS's)." Briefing for the DMS SPWG. Washington, 26 June 1992.

Edmonds, Albert J., Major General, United States Air Force. "Multilevel security Program Issues." Draft Memorandum for the Director, Defense Information Systems Agency. Washington, 1992.

Friedman, A.R., and I.M. Olson. Introduction to Certification and Accreditation Concepts. McLean, Virginia: National Security Agency, June 1992.

Hicks, Cindy K., Chair, DMS Security Policy Working Group. "June SPWG Meeting Minutes." Washington, June 1992.

Hollister, Gregory S., Lieutenant Colonel, United States Air Force. "DCS Initiatives DISN-NT/DMS/ITSDN: How they Interrelate and How they Support C4I for the Warrior." Briefing for the J6 Conference of the CINCs. Washington, June 1992.

Hughes Aircraft. "What is the Applique?" Briefing for the Joint Staff. Washington, October 1992.

Kohlmann, James, Major, United States Army. TPN-DDN Functional Requirements Document Coordinating Draft. Army Draft Document. Ft. Gordon, Georgia: U.S. Army Signal Center, 22 June 1992.

Macke, Richard C., VADM, United States Navy. "Command, Control, Communications and Computers (and Intelligence) for the Warrior." Draft Concept Paper. The Joint Staff. Washington, 27 March 1992.

National Security Agency. Pre-Message Security Protocol. National Security Agency Briefing. Washington: June, 1992.

Stoll, Cliff. The Cuckoo's Egg. New York: Simon and Schuster, 1990.

The Joint Staff. Annex C, National Military Strategy Document. CM-1309-92. Washington: The Joint Staff, 19 June 1992.

The Joint Staff. C2 Functional Analysis and Consolidation Review Panel Report. CM-1127-91. Washington: The Joint Staff, 25 November 1991.

The Joint Staff. C4I for the Warrior, Joint Staff Pamphlet. Washington: The Joint Staff, 12 June 1992.

The Joint Staff. Joint Warfare of the US Armed Forces. Joint Pub 1. Washington: The Joint Staff, 11 November 1991.

The Joint Staff. National Military Strategy of the United States. Joint Staff Pamphlet. Washington: The Joint Staff, January 1992.

The White House. National Security Strategy of the United States. White House Pamphlet. Washington: The White House, August 1991.

U.S. Department of the Army. Army Reserve Forces Policy Committee, Annual Report, 1991. Army Report. Washington: Office of the Secretary of the Army, 31 December 1991.